

REMARKS

This Application has been carefully reviewed in light of the Office Action mailed February 28, 2005. Claims 1-27 were pending in the Application and stand rejected. Applicant amends Claims 1, 4-6, 9-10, 14, 16-17, 19-20, 22-23 and 25-27 to advance prosecution. Applicant requests reconsideration and favorable action in this case.

Amended Claims 1-27 are Allowable.

- Claims 1-3, 5, 7, 14, 15, 18, 20, 21, 24 and 26 are rejected under 35 U.S.C. § 102(b) as being anticipated by PCT Application WO 0070458, by Sheymov et al., published on 11/23/2000 ("*Sheymov*").
- Claims 10-13 are rejected under 35 U.S.C. § 102(e) as being anticipated by US Published Application No. 2004/0003116 to Munger et al. ("*Munger*").
- Claims 4, 6, 9, 16, 17, 19, 22, 23, 25 and 27 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Sheymov* in view of *Munger*.
- Claim 8 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Sheymov* in view of US Published Application No. 2002/0091941 to Challener et al. ("*Challener*").

Applicant respectfully submits that amended Claims 1-27 are allowable at least because the cited references, alone or in combination, fail to teach or suggest each and every element recited in such claims.

For example, amended Claim 1 recites:

A method for securing packet-based communications comprising:
receiving at a first translation module a stream comprising a plurality of packets regarding a communication from a first user interface device intended for a second user interface device, each packet having an original destination address and an original source address; and
for each of the packets, performing an address modification process including changing the original destination address to a selected one of a plurality of modified destination addresses assigned to a second translation module remote from the first translation module, wherein each of the selected modified destination addresses is resolvable by the second translation module to the original destination address for forwarding the packet to the second user interface device;
wherein the address modification process is performed independently from both the first user interface device and the second user interface device.

Among other elements, the cited references, alone or in combination, fail to teach or suggest:

- receiving at a first translation module a stream comprising a plurality of packets regarding a communication from a first user interface device intended for a second user interface device . . .
- performing an address modification process including changing the original destination address to a selected one of a plurality of modified destination addresses . . . resolvable by the second translation module . . . [and]
- wherein the address modification process is performed independently from both the first user interface device and the second user interface device (emphasis added)

In other words, the cited references, alone or in combination, fail to teach or suggest modifying addresses for packets of a communication between user interface devices, wherein the address modification process is performed independently from both of the user interface devices. In contrast, the cited references disclose address modification performed by at least one of the user interface devices involved in the communication.

First, *Sheymov* teaches a system for protecting against unwanted network intrusion in which the cyber coordinates of a protected computer 14 are changed both on a determined time schedule and when an intrusion attempt is detected. (Abstract). A management unit 18 generates a random sequence of cyber coordinates and maintains a series of tables containing the current and next set of cyber coordinates. (Abstract). These cyber coordinates are then encrypted and distributed to authorized users to prevent unauthorized access. (Abstract; Page 3, lines 20-27). Thus, as shown in Figures 1, 3 and 5 of *Sheymov*, an authorized user (remote user 12) receives a set of cyber coordinates and performs the process of changing the cyber coordinates of the protected computer over time. Thus, remote user 12 is integrally involved in the address changing process, and therefore, the system disclosed by *Sheymov* cannot provide the advantages of the independently-provided address modification recited in amended Claim 1, which advantages are discussed below.

Second, *Munger* teaches a system for establishing secure communications between a client computer 801 and a TARP router 811. (Paragraph 0112; Figure 8). The client computer 801 sends the router 811 an authentication token. (Paragraph 0112; Figure 8). In response, the router 811 sends “hopblocks” to the client computer 801, which include blocks of IP addresses and address-change algorithms appropriate for communicating with the router 811. (Paragraphs 0108, 0109, 0112; Figure 8). The client computer 801 then uses the block of IP addresses and address-change algorithms to communicate securely with the router 811. Thus, the client computer 801 is integrally involved in providing the address-hopping functionality. Therefore, like *Sheymov*, *Munger* cannot provide the advantages of the independently-provided address modification recited in amended Claim 1, which advantages are discussed below.

Third, *Challener* does not teach or suggest address modification at all, much less address modification performed independently from the user interface devices involved in a communication.

Providing security-related address modification independently from the user interface devices involved in the particular communication provides several advantages over providing address modification by the user interface devices themselves. First, because the address modification is performed independently from the user interface devices involved in the communication, the address modification may be performed anywhere in the network. For example, as shown in Figure 1 of Applicant’s disclosure, the address modification may be performed by translation modules 12 located between portions of a PSTN network 16 and an IP network 28. Thus, as discussed in Applicant’s Specification, such translation modules 12 may be used to perform address modification for packets that have already passed through a portion of a PSTN network 16 and have been converted from circuit-switched communications into packets by a media gateway 24. Thus, such address modification may be used to provide security for communications that originated as circuit-switched communications, such as telephone calls passing through a PSTN network, for example. In contrast, systems in which address modification is performed by one or both of the user interface devices themselves, such as the systems disclosed by *Sheymov* and *Munger*, cannot provide such functionality.

In addition, because the address modification is performed independently from the user interface devices in a network, a single translation module 12 may perform the address translation for any number of user interface devices connected to that translation module 12. For example, as shown in Figure 1 of Applicant's disclosure, a translation module 12 may provide address modification functionality for any number of telephones 14 connected to a PSTN central office 18. In contrast, in systems in which address modification is performed by one or both of the user interface devices themselves, such as the systems disclosed by *Sheymov* and *Munger*, each user interface device must provide its own address modification functionality, which may require additional hardware and/or software for each user interface device.

For at least these reasons, Applicant respectfully requests reconsideration and allowance of amended Claim 1, together with Claims 2-9 that depend from therefrom. In addition, for analogous reasons, Applicant respectfully requests reconsideration and allowance of amended independent Claims 10, 14, 20, 26 and 27, together with Claims 11-13, 15-19 and 21-25 that depend from Claims 10, 14 and 20.

Conclusions

Applicant has made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicant respectfully requests full allowance of all pending Claims. If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, the undersigned attorney for Applicant stands ready to conduct such a conference at the convenience of the Examiner.

No fees are believed to be due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant



Kurt M. Pankratz
Reg. No. 46,977

Date: May 31, 2005

Customer Number:

05073